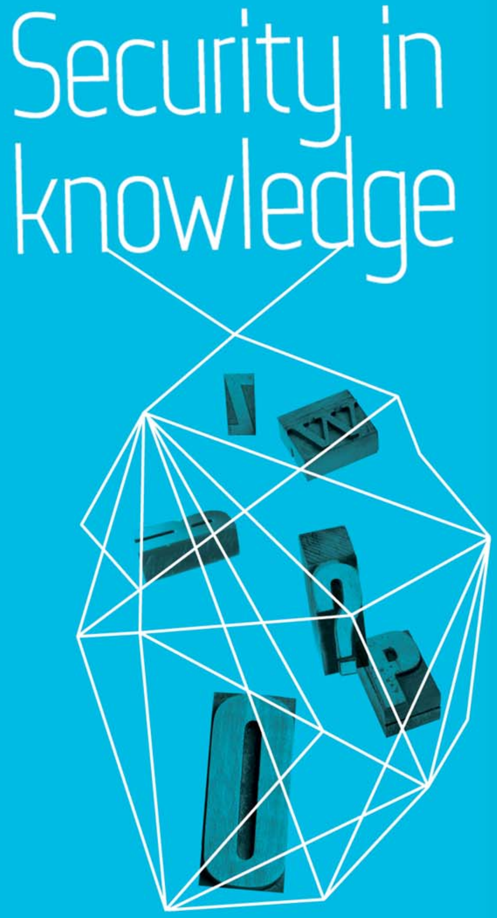
RSACONFERENCE2013



ADAPTING OAUTH TO THE ENTERPRISE

Chuck Mortimore
salesforce.com

Pat Patterson
salesforce.com

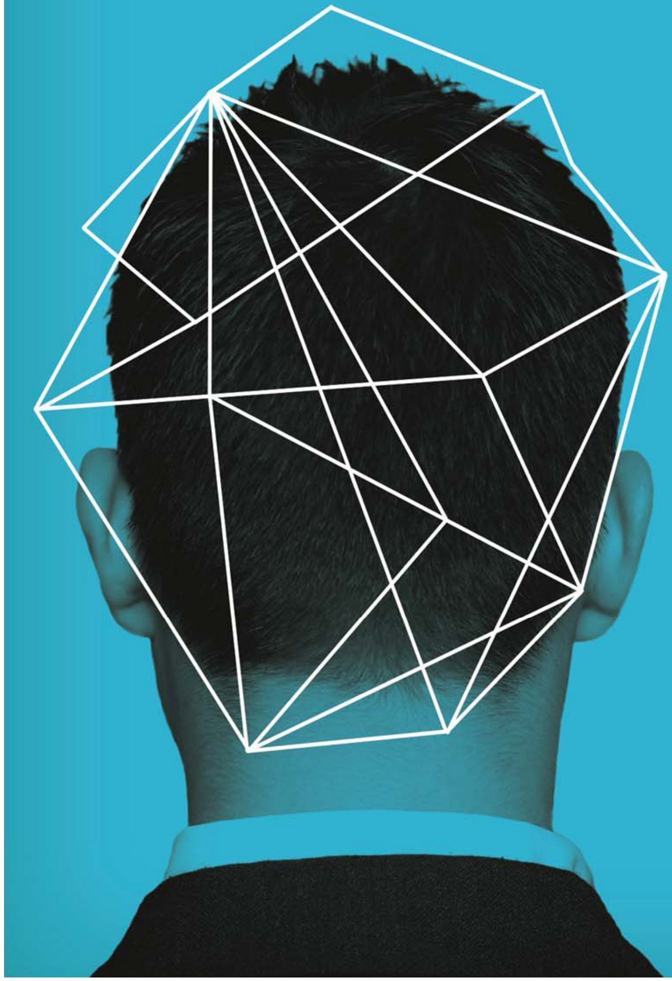
Session ID: IAM-F42A

Session Classification: Intermediate

AGENDA

- OAuth recap
- OAuth for consumers
- OAuth for enterprises
- OpenID Connect
- What’s next?
- Q&A

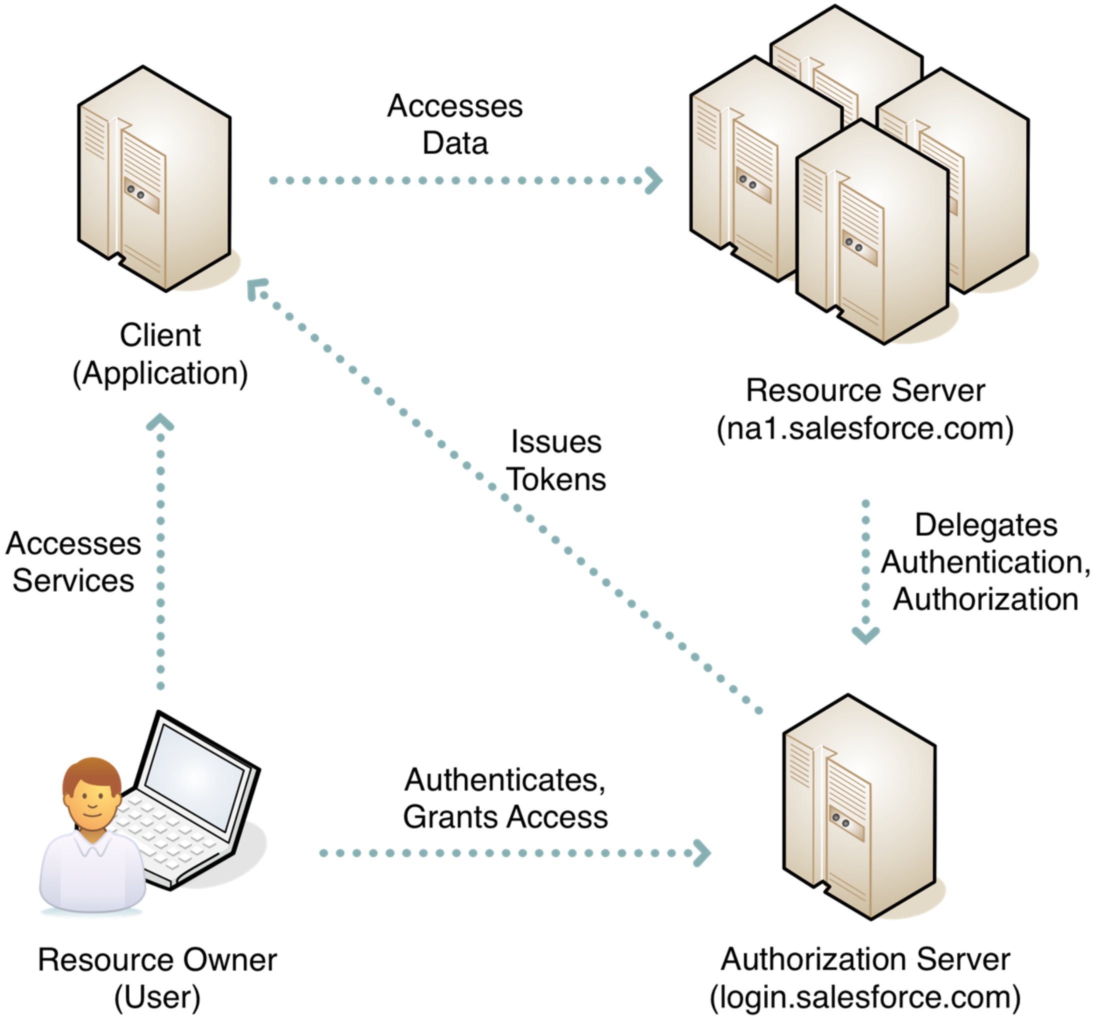
OAUTH 2.0



OAUTH 2.0

- Authorization for 'HTTP services' (e.g. RESTful APIs)
- Evolution of Google AuthSub, Yahoo BBAuth, AOL OpenAuth etc
- RFCs 6749/6750 (October 2012)

OAUTH 2.0 ROLES

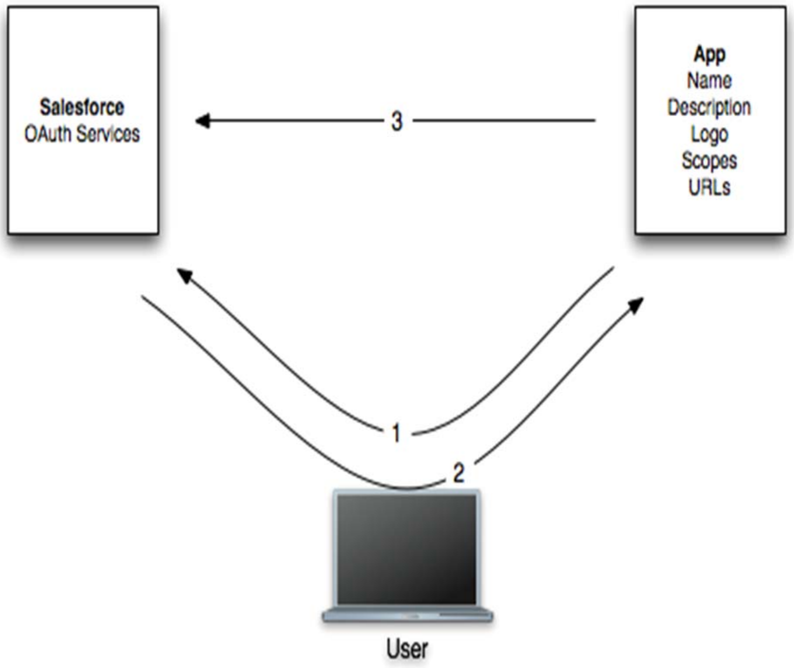

Accesses Data
Client (Application)
Resource Server (na1.salesforce.com)
Issues Tokens
Accesses Services
Delegates Authentication, Authorization
Authenticates, Grants Access
Resource Owner (User)
Authorization Server (login.salesforce.com)

CODE FLOW: HOW DOES IT WORK?

- App Redirects User to Authorization Services where User is Authenticated and Authorizes App

- Code Returned to App

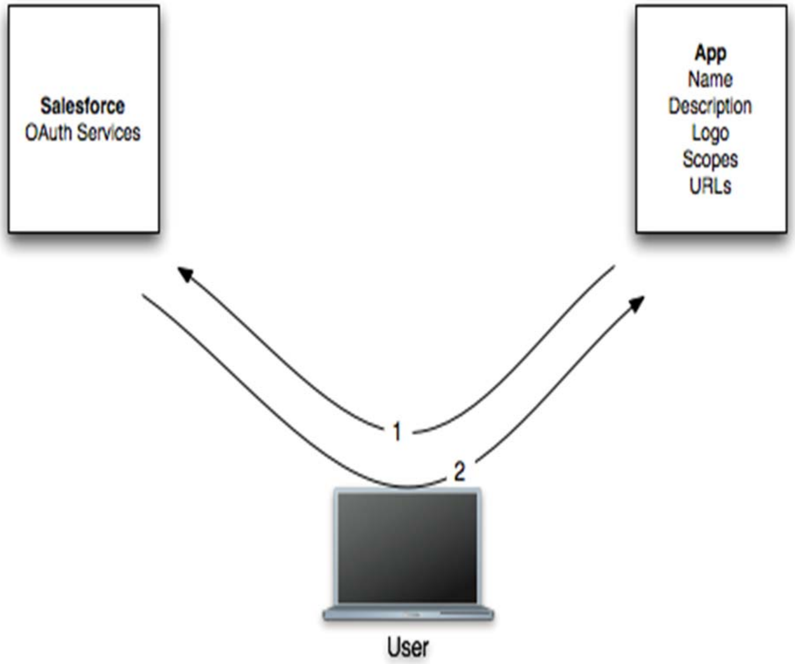
- App Exchanges Code at Token Service



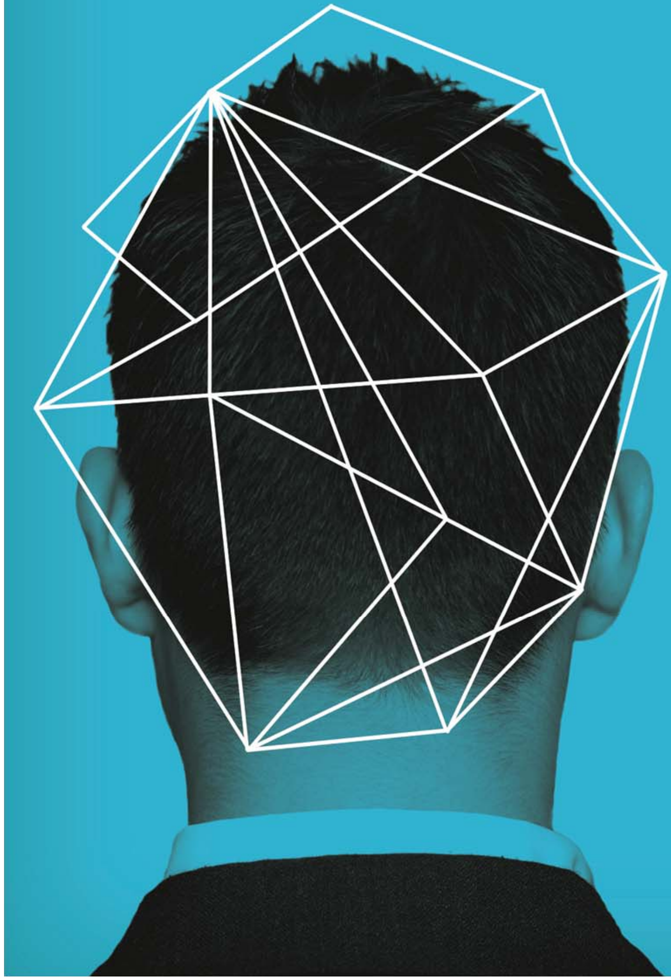
TOKEN FLOW: HOW DOES IT WORK?

- App Redirects User to Authorization Services where User is Authenticated and Authorizes App

- Token Response returned directly to app on URL behind a # fragment

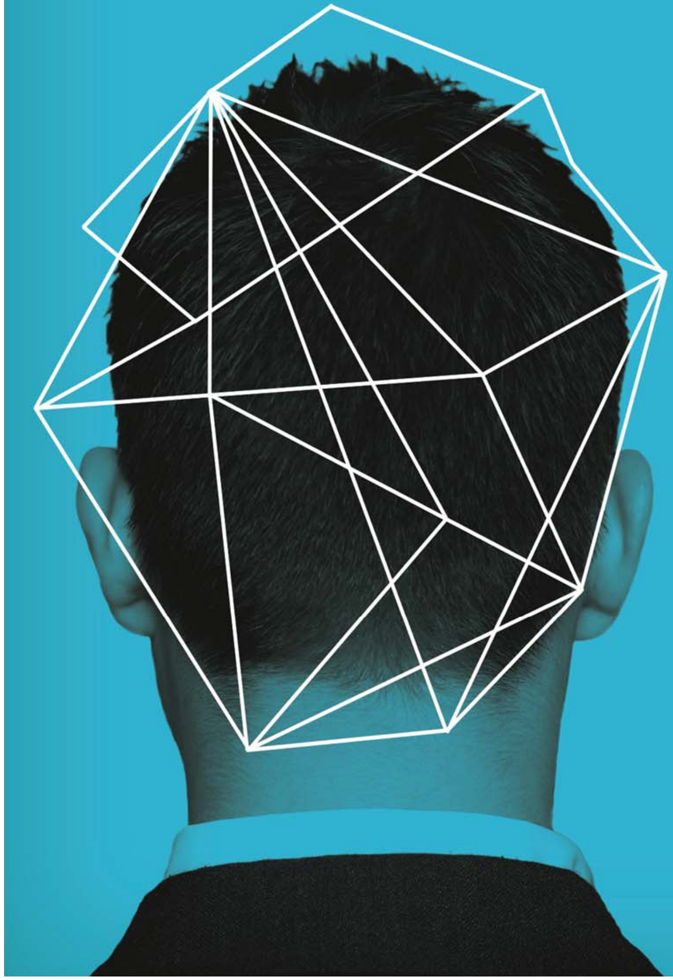


DEMO



RSA CONFERENCE 2013

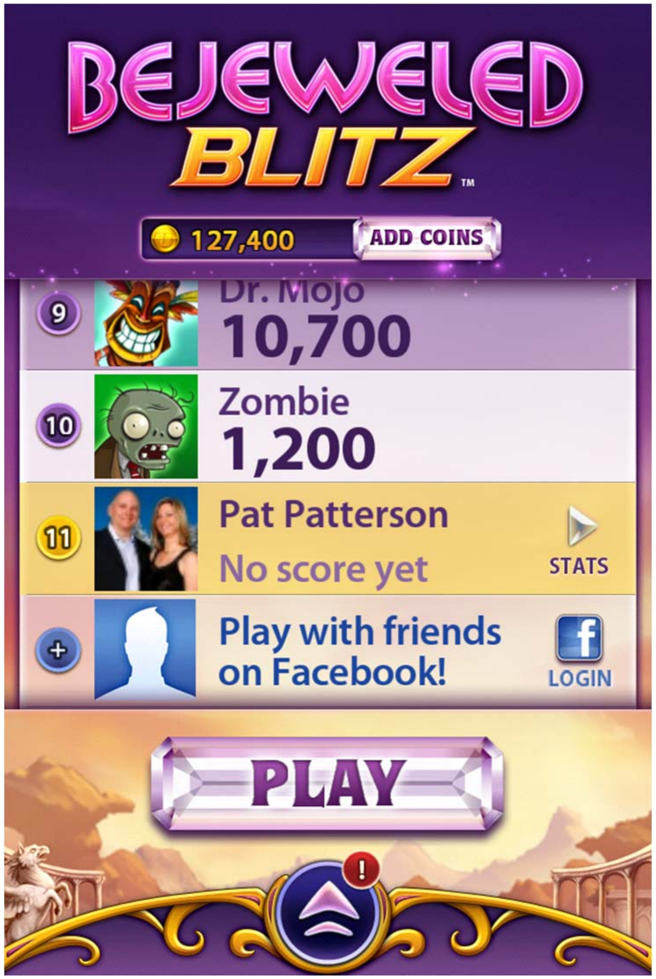
THE CONSUMER EXPERIENCE



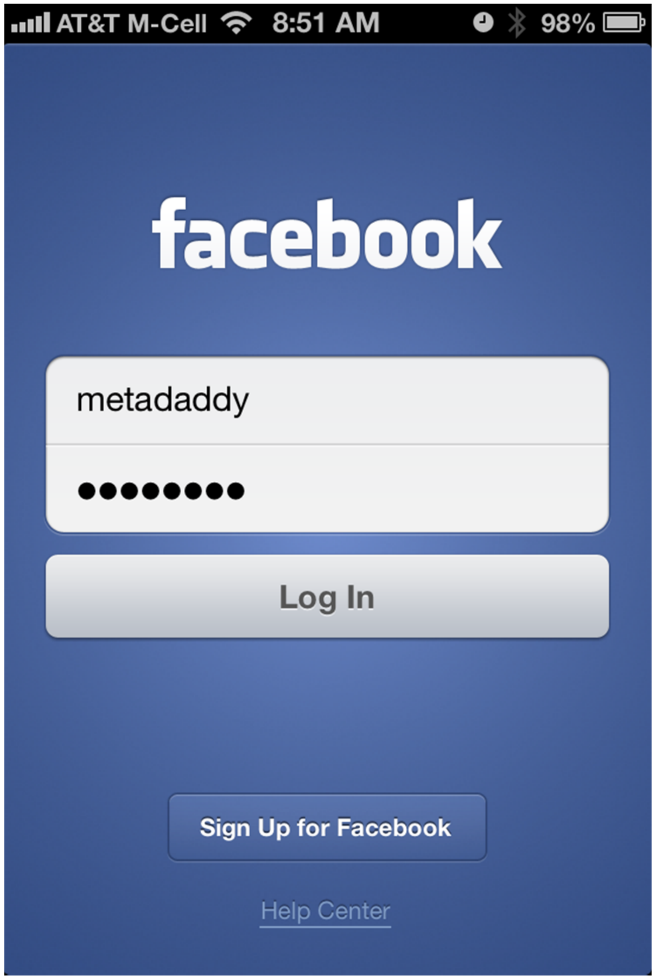
FACEBOOK

- Early adopter (draft 12, Sep 2010)
- Client-side JavaScript SDK, Native Device = Implicit Grant Flow
- Server-side = Authentication Code Flow
- Probably the biggest OAuth 2.0 deployment in the world

CONSUMER EXPERIENCE



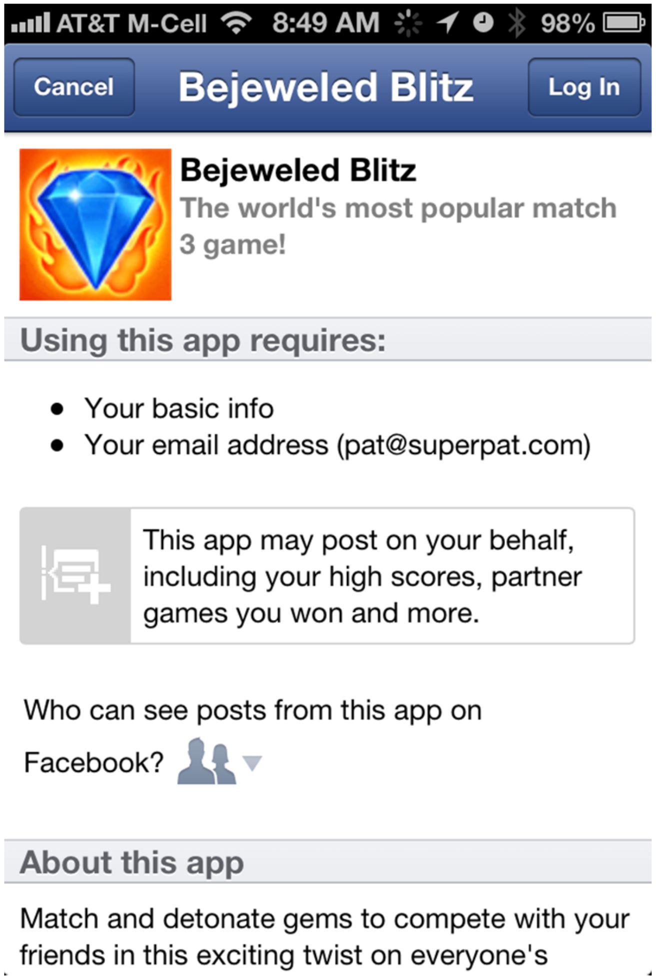
CONSUMER EXPERIENCE



metadaddy

●●●●●●●●

CONSUMER EXPERIENCE



Bejeweled Blitz

The world's most popular match 3 game!

Using this app requires:

- Your basic info
- Your email address (pat@superpat.com)

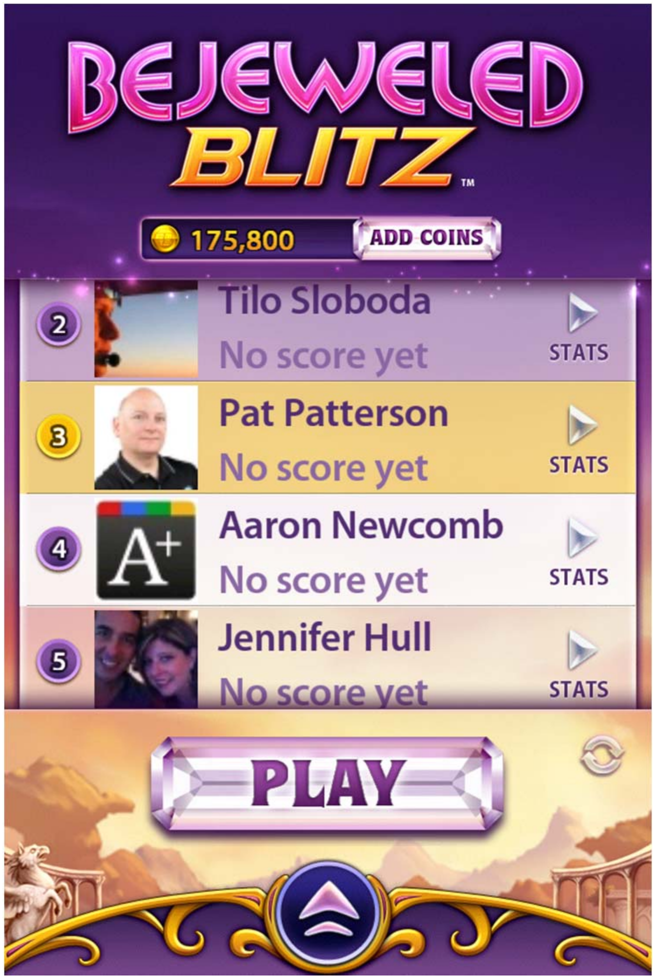
This app may post on your behalf, including your high scores, partner games you won and more.

Who can see posts from this app on Facebook?

About this app

Match and detonate gems to compete with your friends in this exciting twist on everyone's

CONSUMER EXPERIENCE



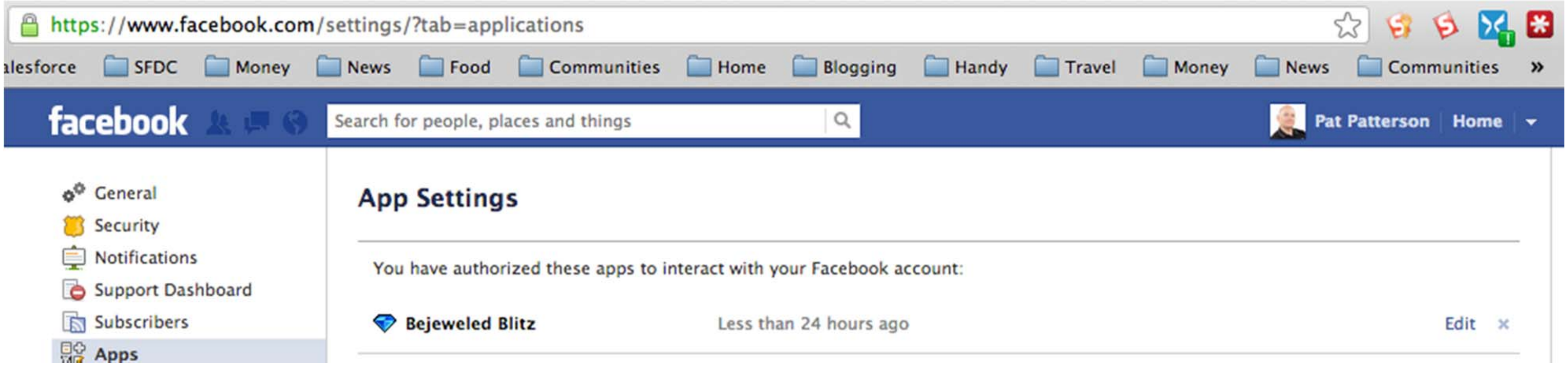
2 Tilo Sloboda
No score yet

3 Pat Patterson
No score yet

4 Aaron Newcomb
No score yet

5 Jennifer Hull
No score yet

CONSUMER EXPERIENCE



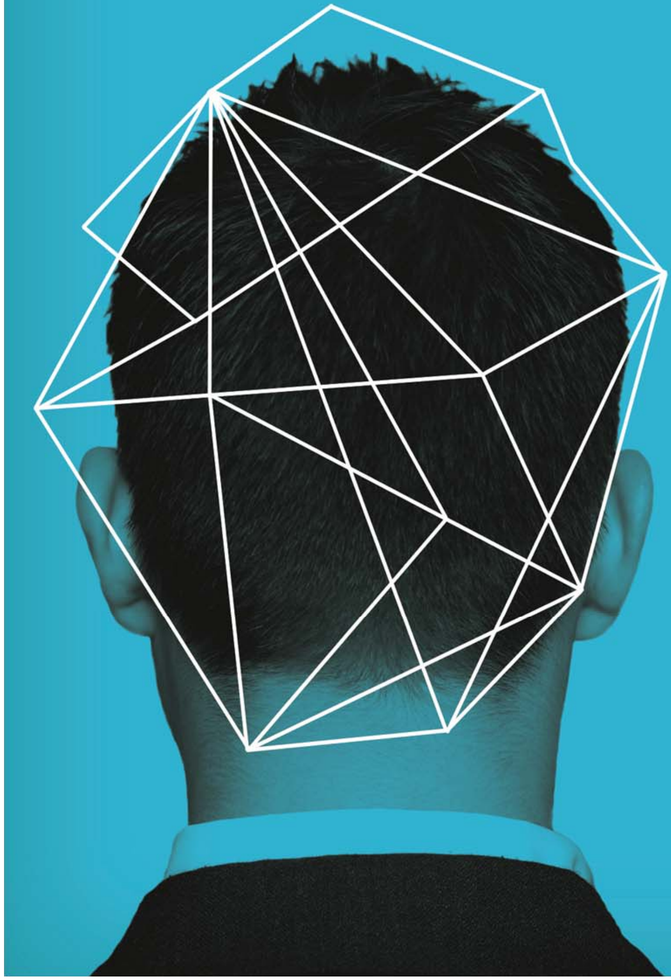
https://www.facebook.com/settings/?tab=applications

App Settings

You have authorized these apps to interact with your Facebook account:

Bejeweled Blitz — Less than 24 hours ago — Edit ×

RSA CONFERENCE 2013



ADAPTING OAUTH 2.0 TO THE ENTERPRISE

WHY WE LOVE OAUTH

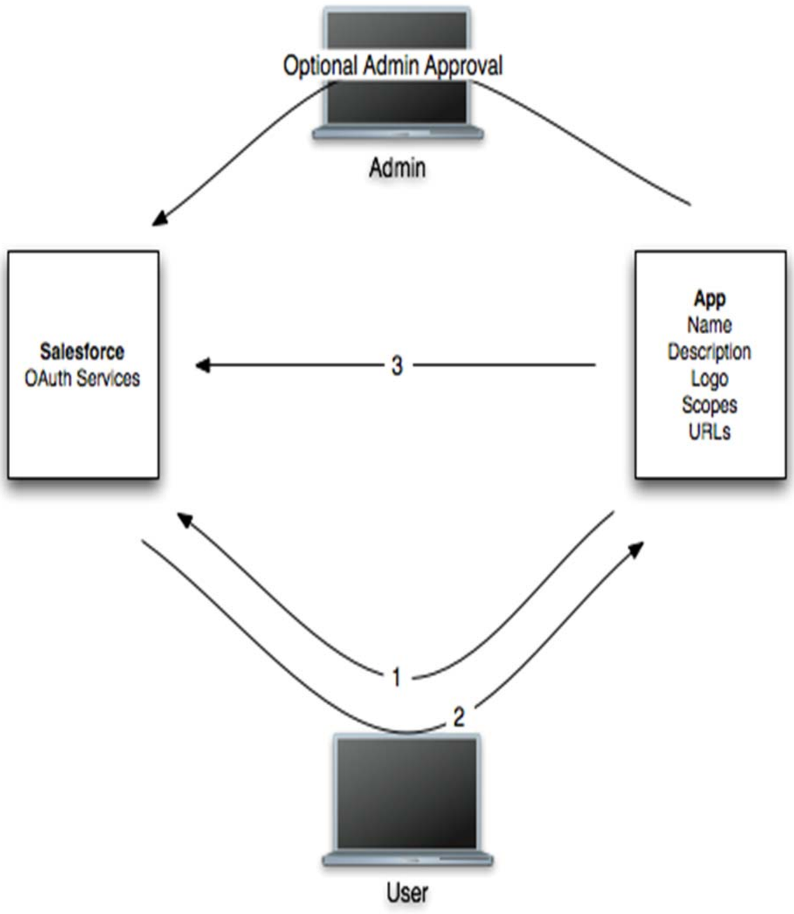
- Simple Developer Experience
  - Approachable without massive investment
- Mobile Optimized
  - This is where your business processes are going
- Broad platform applicability
  - It’s just HTTP
- Adaptive Authentication
  - Allows us to leverage the web
- Context
  - Adds Application as an actor

WHAT THE ENTERPRISE DOESN'T LOVE

- Consumer Authorization
  - Who has jurisdiction over enterprise resources?
- Uncontrolled Mobile Devices
  - How do gain control over where credentials are used?
- Passwords
  - What about assertions, token services, and federation?
- Server to Server
  - What if I don't have a "user"?

ADMIN AUTHORIZATION

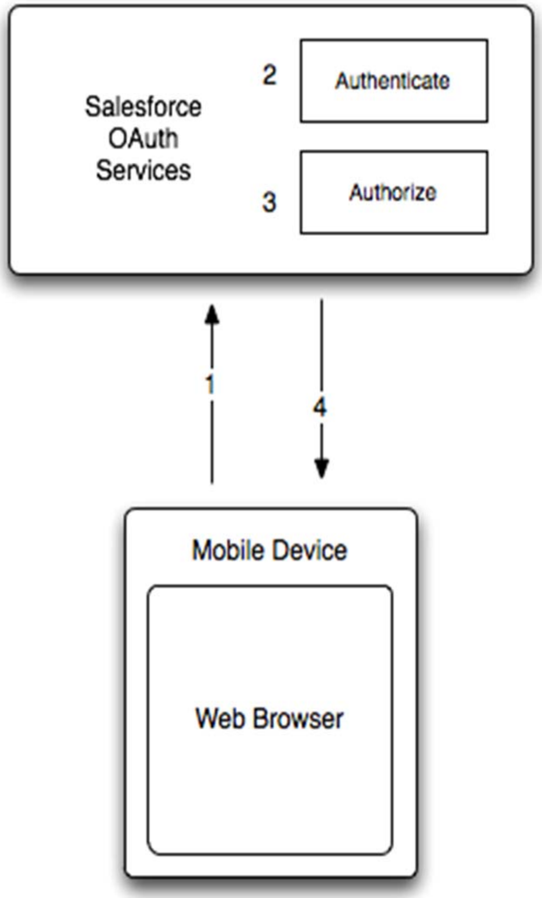
- Admin “installs” app
- App Uses any OAuth Flow
- User Authorization is determined via Admin settings
- Optional Policy Enforcement



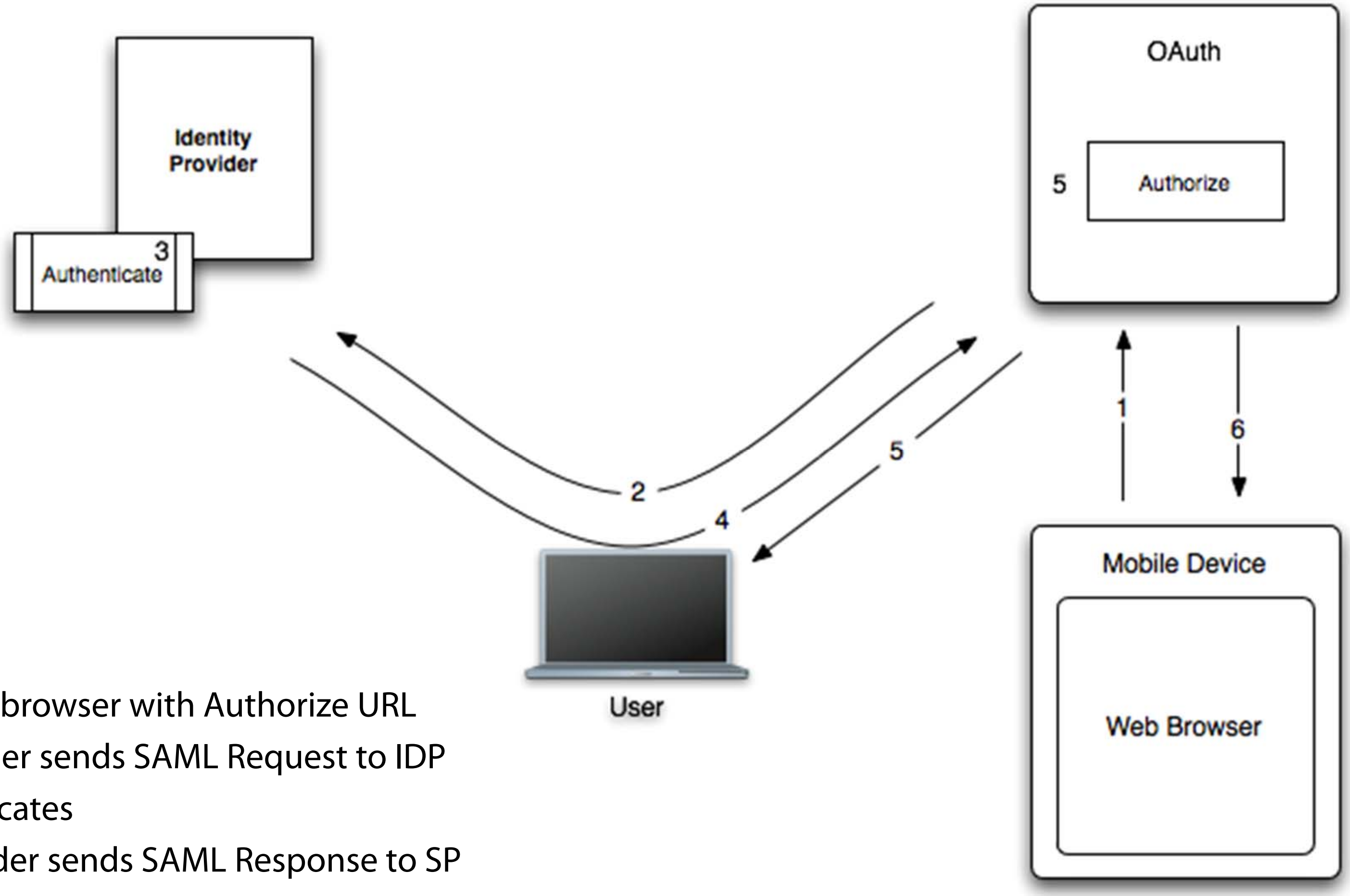
MOBILE

- Device opens a browser with authorization URL

- Tokens returned on URL behind # fragment – instrumented browser is monitoring and parses URL



MOBILE FEDERATION

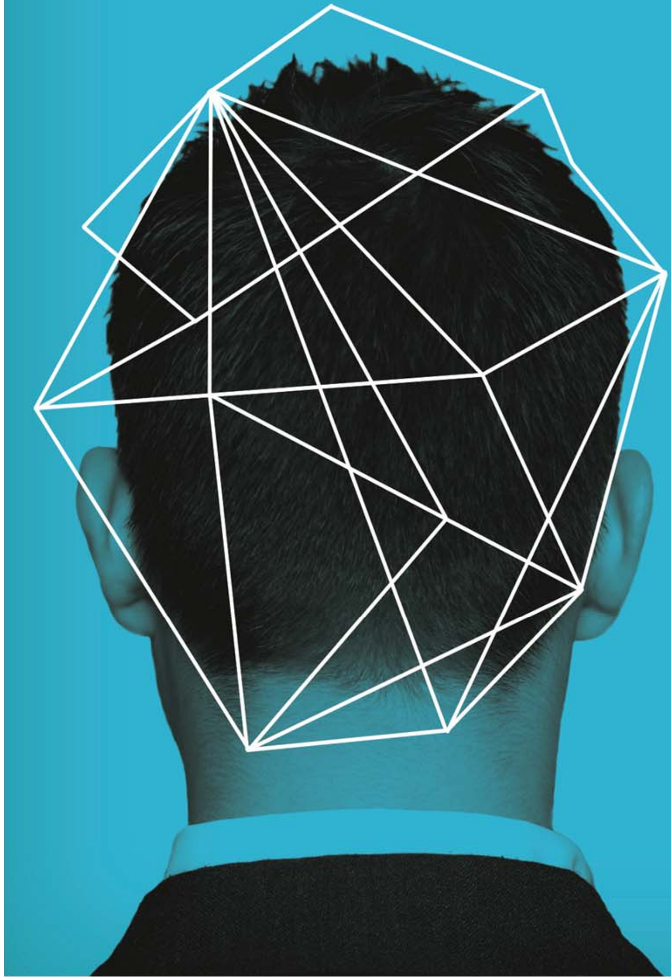


- 1 - Device opens browser with Authorize URL
- 2 - Service Provider sends SAML Request to IDP
- 3 - User Authenticates
- 4 - Identity Provider sends SAML Response to SP
- 5 - OAuth request is Authorized
- 6 - Authorization Service responds with code or Token Response

SERVER TO SERVER OAUTH

- RESTful STS Pattern
  - Apps can exchange Credentials or Assertions for API tokens
  - Enables API Federation, and password-less Cloud
- Username / Password Flow
  - Simple, but uses passwords
- Web SSO Assertion Flow
  - Reuse SAML SSO and existing Trust
- SAML/JWT Assertion Flow
  - Cert and Trust Specific to the App

FUTURES

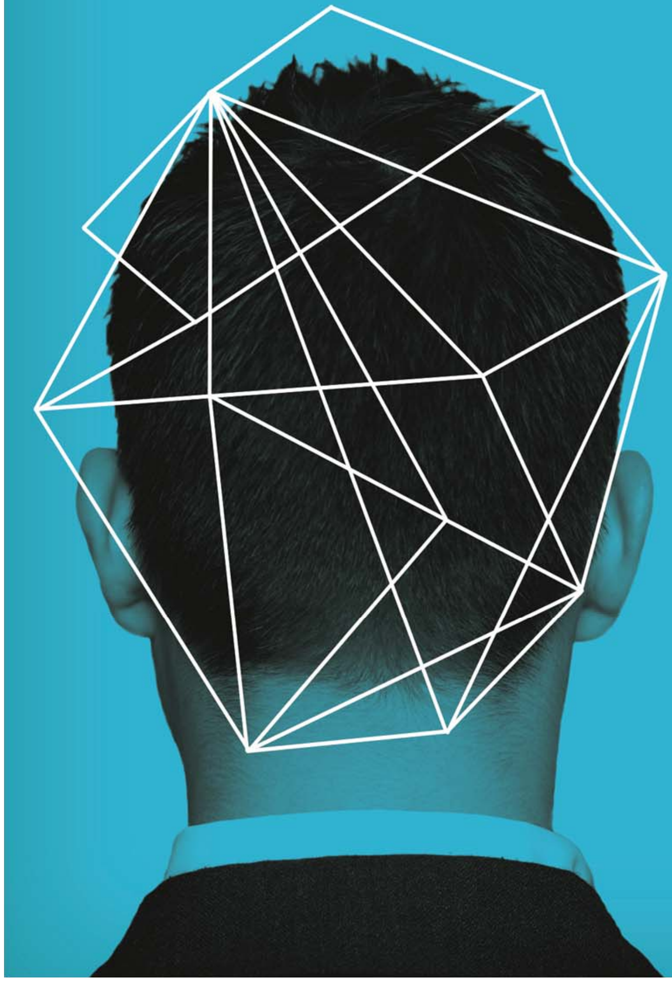


WHERE IS THIS HEADING?

- Complete the standardization of Assertion Flows
  - http://tools.ietf.org/html/draft-ietf-oauth-assertions-09
  - http://tools.ietf.org/html/draft-ietf-oauth-saml2-bearer-15
  - http://tools.ietf.org/html/draft-ietf-oauth-jwt-bearer-04

- Mobile App Federation

RSACONFERENCE2013



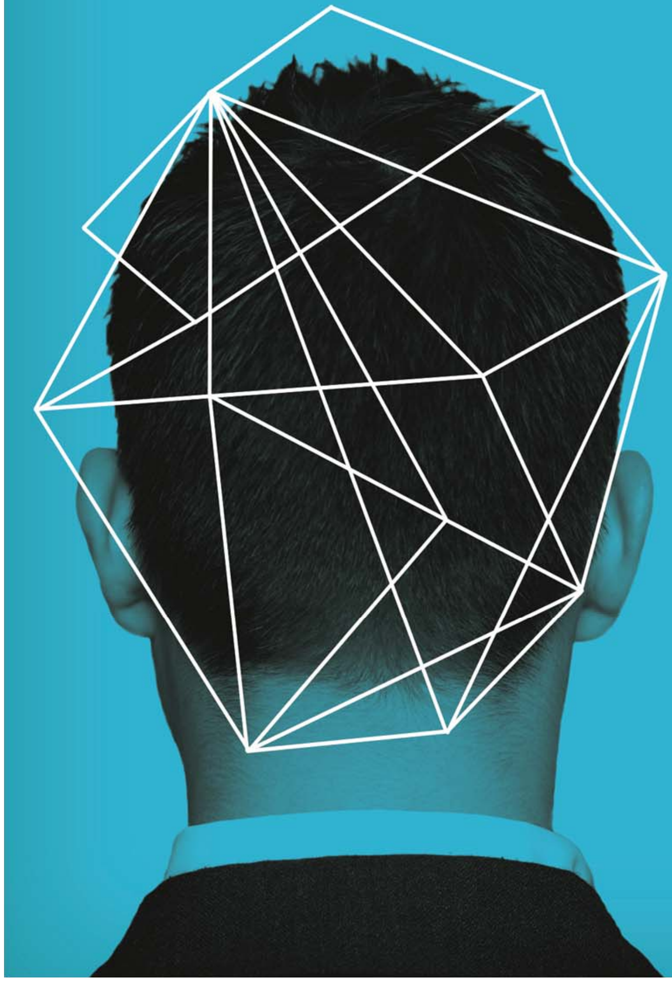
SUMMARY

SUMMARY

- OAuth 2.0…
  - is now an IETF standard (RFC 6749)
  - minimizes password proliferation
  - enables apps to access APIs on behalf of millions of consumers and enterprise users every day

RSACONFERENCE2013

Q & A



Chuck Mortimore
cmortimore@salesforce.com

Pat Patterson
ppatterson@salesforce.com